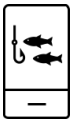
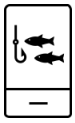


Mobile Phishing Attacks on Australian Government



Overview

The Australian government has confirmed that a series of mobile phishing attacks were successfully executed on targeted senior diplomats. The campaigns targeted members of Parliament with messages that asked them to validate new WhatsApp or Telegram accounts. Once the attack was successfully executed and the threat actor stole the target's login credentials, they gained access to the target's address book and could send messages out on their behalf. The attacker seemed particularly interested in finding out if the targets had any contacts in Hong Kong.

Lookout Analysis

This incident shows that phishing campaigns do not have to be complex in order to be effective. Something as simple as asking an individual to validate their account can be a highly effective form of social engineering. Since the mobile device is so frequently used as an additional form of authentication or validation, we've grown accustomed to not thinking twice about receiving an account validation message via SMS, WhatsApp, Telegram, Facebook Messenger, or any other communication app.

Mobile devices are seen as an extension of the individual user, which is why people trust them to be inherently secure. Government officials, like any other workers, may conduct business across both sanctioned and personal apps. With the same strategy used in this incident, an attacker could just as easily get a government official to download a malicious version of a messaging app that's laced with surveillanceware, spyware, or other highly invasive tracking or data exfiltration malware.

Lookout Coverage and Recommendation for Admins

Lookout Phishing & Content Protection will help protect mobile users from malicious phishing campaigns built to exploit these vulnerabilities. Lookout PhishingAI constantly monitors the web for new sites built specifically for phishing purposes and implements protection against them in near real-time.

Lookout admins can force activation of Phishing & Content Protection on their employees' devices by not allowing them to access corporate resources or cloud infrastructure until the capability is enabled

Lookout Phishing & Content Protection

As part of the broader endpoint-to-cloud security solution, Lookout provides comprehensive mobile phishing protection on both Android and iOS devices. This gives admins powerful tools for monitoring, managing and protecting mobile devices, and enables organizations to confidently embrace the use of smartphones within their organization.

Click here to learn more about Phishing & Content Protection